

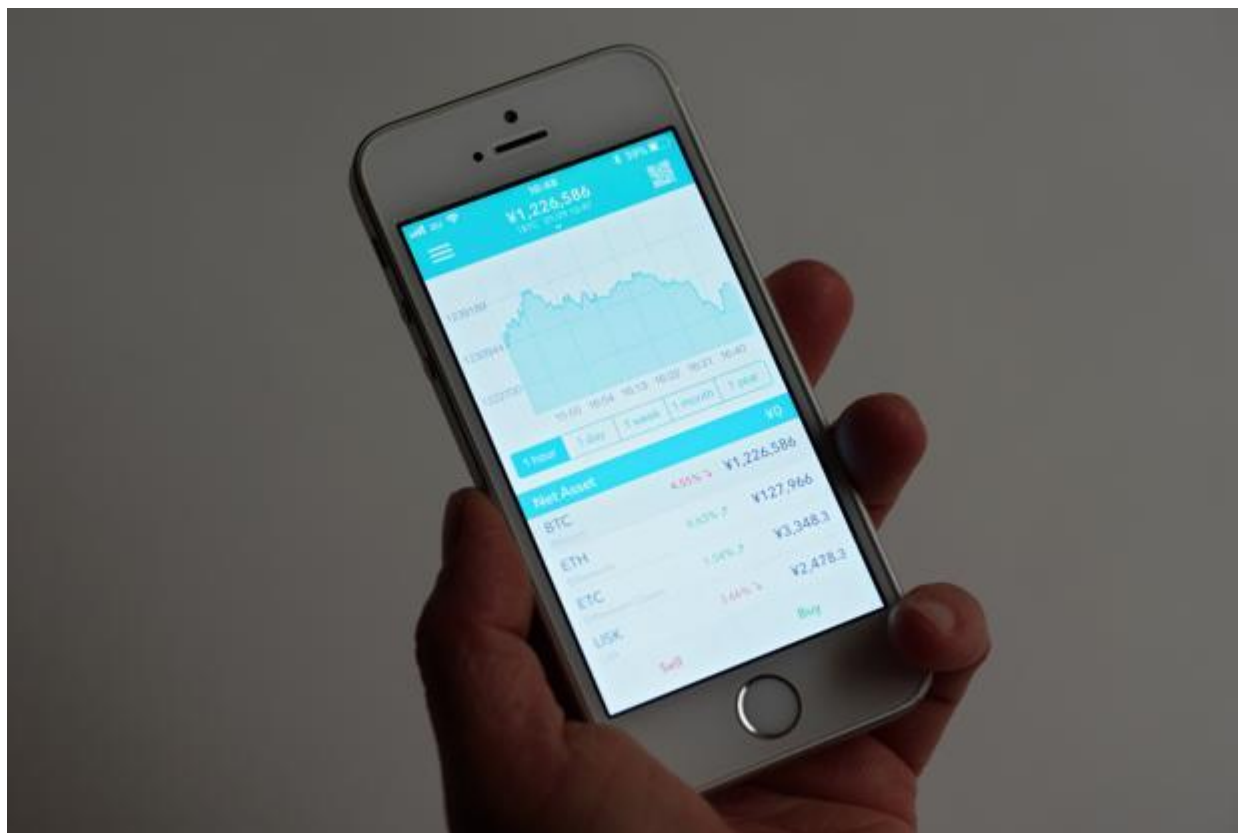
[Home » Industry](#)

Record crypto heist raises the appeal of a new type of exchange

Called decentralized exchanges, the newfangled markets being developed or already deployed by AirSwap, EtherDelta and others sidestep that vulnerability by giving up the vault entirely

Last Published: Tue, Jan 30 2018. 12 14 PM IST

Olga Kharif

[Sign Up](#)

Last week, half a billion dollars of a currency called NEM was purloined from Coincheck Inc., one of Japan's biggest cryptocurrency exchanges. Photo: Bloomberg

Get Notifications

Portland: A more than \$500 million record heist from a Japanese cryptocurrency exchange, the latest in a long line of high-profile hacks, is directing attention to a new kind of venue that makes it harder for would-be thieves. They're not, however, impervious to attack.

Hackers typically steal money from crypto exchanges by gaining access to their internet-connected wallet, which stores the funds of customers. Hackers have repeatedly cracked open the virtual vaults where they're stashed, stealing billions of dollars worth of assets over the years.

Called decentralized exchanges, the newfangled markets being developed or already deployed by AirSwap, EtherDelta and others sidestep that vulnerability by giving up the vault entirely. Instead, their customers keep their private keys, needed to access their accounts, and transact with each other directly, or with minimal help.

Last week, half a billion dollars of a currency called NEM was purloined from Coincheck Inc., one of Japan's biggest cryptocurrency exchanges. This incident provides "more evidence that the crypto-infrastructure should move away from centralized custody-type exchanges to decentralized exchanges where the need to have a middleman function is no longer necessary," said David Shin, a founding member of the Bitcoin Association of Hong Kong and president of the Singapore-based Asia Fintech Society.

Their security isn't bulletproof.

In December, a hacker hijacked EtherDelta's website, replacing it with a fake version that let the thief steal users' funds.

Even the ultra-rich go to extreme lengths to keep their private keys safe. Cameron and Tyler Winklevoss, who were briefly Bitcoin billionaires last year because of the currency's huge surge, told the *New York Times* in an interview published in December about their low-tech solution: printing out their passcodes, cutting them into pieces and stashing the parts in safe deposit boxes around the nation.

Because the exchange usually doesn't verify users' identity, it's harder to recover stolen funds: After all, blockchain is designed to be an immutable record.

"If a rogue transaction happens in a decentralized exchange, there is no way to revert the transaction," said Matt Suiche, founder of security provider Comae Technologies. "You may trace a criminal until they jump to another cryptocurrency, and then you can easily lose track of them."

Some think the kinks will eventually get worked out.

“It is very possible that one day the majority of the volume will be coming from decentralized exchanges,” said Lucas Nuzzi, a senior analyst at Digital Asset Research. “Before that happens, however, many issues regarding the way Decentralized Autonomous Organizations are regulated, taxed and insured need to be solved. Having said that, it is remarkable that millions of dollars worth of digital tokens flow through these exchanges every month.”

New decentralized exchanges are popping up rapidly. Seven exchanges based on technology called ox went online since the fall, and at least five more will launch soon.

Radar Relay, which launched in October and counts Blockchain Capital among its investors, has facilitated almost \$40 million in transactions in the past month, according to otracker.com.

“It’s tough to get folks to jump ship for the decentralized exchange, and we recognize that,” said Alan Curtis, chief executive officer at Radar. “But folks are fleeing because of hacks.”

ShapeShift, which handles up to 35,000 decentralized trades a day, brags about the time it was hacked in 2016. That’s because no user funds were taken.

“It was a very good use case to tell our customers, ‘Hey we were hacked, and it didn’t affect any of you,’” a company spokeswoman said in a phone interview. ShapeShift hedges itself against the broader risk of hacks by not allowing employees to give out the last names. **Bloomberg**

First Published: Tue, Jan 30 2018. 10 30 AM IST

TOPICS:

CRYPTOCURRENCY

BITCOIN

COINCHECK

JAPAN

DECENTRALIZED EXCHANGE

You May Like

Sponsored Links by Taboola

Don't Pay More Than This For a 4-Star Hotel Room

save70.com

Want To Be Own Boss In 2017? Start An Online Business In Your Spare Time!

Project Ignite

Play this Game for 1 Minute and see why everyone is addicted

Delta Wars

Gorgeous Siblings You Didn't Know These Celebrities Had

Hooch

Surprising Rewards For People Born Between 1941 - 1981

Survey Compare

4 things parents should stop doing immediately

Lifetrendsy

[EDITOR'S PICKS »](#)

Get Notifications



PNB fraud effect: Modi govt’s anti corruption crusade goes into overdrive



How to break the banker-promoter nexus



Boeing makes a pitch for F/A-18s to India

Home

Lounge

Specials

Companies

Multimedia

Technology

Opinion

Money

Mint on Sunday

Industry

Science

Contact Us

Politics

Education

About Us

Consumer

Sports

Advertising

Sitemap

Brand Stories

DesiMartini

Livehindustan

Mint Apps

Subscribe

Shine

Hindustantimes

Syndication

Get Notifications

Subscribe to our Newsletter

[Privacy Policy](#)

[Terms of Use](#)

[Mint Code](#)

[RSS](#)

Copyright © 2018 HT Media Ltd. All Rights Reserved